UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,455	11/17/2003	Kazuya Suzuki	8022-1063	2290

466 7590 12/23/2008

YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
ZEE, EDWARD	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,455	SUZUKI ET AL.	
	Examiner	Art Unit	
	EDWARD ZEE	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendments filed on August 22nd, 2008. Claims 1 and 12-17 have been amended; Claims 1-19 are pending and have been considered below.

Claim Objections

2. The amendments filed on August 22nd, 2008 have been considered and are effective at overcoming the previous claim objections, and thus have been withdrawn.

Claim Rejections - 35 USC § 112

3. The amendments filed on August 22nd, 2008 have been considered and are effective at overcoming the previous claim rejections, and thus have been withdrawn.

Claim Rejections - 35 USC § 102

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-4, 18 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Briscoe (2003/0044017).

Claim 1: Briscoe discloses a multicast delivery system comprising:

a. a delivery server*(ie. data sender)* which enciphers delivery data by using a current use cipher key to generate enciphered data and transmits a multicast packet containing said enciphered data and a current use key identifier*(ie. key sequence)* indicative of a pair of said

current use cipher key and a current use decipher key as current use keys*(ie. data sender issues seed values)* [page 3, paragraph 0061];

b. a key management server*(ie. key management node)* which is connected with said delivery server through a network, holds as a current use key data*(ie. key management application receives seed values from data senders)*, a set of said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data in response to a current use key data request*(ie. issues seed values to customer terminals)* [page 3, paragraph 0061];

c. and a client terminal which is connected with said delivery server and said key management server through said network, receives said multicast packet from said deliver server, issues said current use key data request to said key management server to receive said current use decipherment key data from said key management server, holds said set of said current use decipher key and said current use key identifier, and deciphers said enciphered data contained in said multicast packet by using said current use decipher key when said current use key identifier contained in said multicast packet is coincident with said current use key identifier held in said client terminal*(ie. key management node issues customer seed values to allow customers to generate keys corresponding to the key used to encrypt the data)* [page 3, paragraph 0058].

Claim 2: Briscoe discloses the multicast delivery system according to claim 1, and further discloses that said delivery server generates*(ie. key generation sub-module generates a sequence of keys)* and holds as a current use encipherment key data, a set of said current use cipher key, said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as said current use decipherment key

data to said key management server, and said key management server holds said current use decipher key and said current use key identifier as said current use decipherment key data [page 3, paragraph 0062].

Claim 3: Briscoe discloses the multicast delivery system according to claim 2, and further discloses that said delivery server sets a current use key remaining effective time data*(ie. the key is changed every game-minute)* to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use decipherment key data to said key management server, said key management server holds said current use decipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses*(ie. time keeper signals new game-minute)* [pages 4 & 5, paragraphs 71 & 80].

Claim 4: Briscoe discloses the multicast delivery system according to claim 3, and further discloses that said delivery server generates*(ie. increments ADU index to use next key in sequence)* as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data, when said current use key remaining effective time data becomes a first present value*(ie. time-keeper signals a new game-minute)*, and transmits a set of said next use decipher key, said next use key identifier, and said next use key remaining effective time data to said key management server as a next use decipherment key data, and said key management server holds said next use decipher key data*(ie. key managers synchronize by receiving the*

changing stream of ADU sequence numbers from the multicast) [page 5, paragraphs 0080 & 0082].

Claim 18: Briscoe discloses the multicast delivery system according to claim 1, and further discloses that said key management server detects a data amount of said multicast packets and charges a fee to said client terminal based on said detected data amount*(ie. pre-purchase a limited amount of video program material)* [page 1, paragraph 0001].

Claim 19: Briscoe discloses the multicast delivery system according to claim 1, and further discloses that said client terminal issues said key data request to said key management server, and said key management server detects the number of said key data requests and charges a fee to said client terminal based on said detected number of key data requests*(ie. charges per game-minute)* [page 4, paragraph 0069].

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 5-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (2003/0044017) in view of Larsen et al. (7,068,791).

Claim 5: Briscoe discloses the multicast delivery system according to claim 4, and further discloses that said client terminal issues a key request to a key management server*(ie. issues seed values to customer terminals)* [page 3, paragraph 0061], but does not explicitly disclose that a next use key request to said key management server when said current use key remaining

effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

However, Larsen et al. discloses a similar system and further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 6: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 5, but Briscoe does not explicitly disclose that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

However, Larsen et al. further discloses that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0*(ie. current key is used until it expires)* [column 4, lines 15-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in

order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 7: Briscoe discloses the multicast delivery system according to claim 1, and further discloses the delivery server generating current use key data*(ie. key generation sub-module generates a sequence of keys)* [page 3, paragraph 0062], but does not explicitly disclose that said delivery server issues a current use key data generating request to said key management server, said key management server generates and holds as a current use key data, a set of said current use cipher key, said current use decipher key and said current use key identifier in response to said current use key data generating request, and transmits a set of said current use cipher key and said current use key identifier as a current use encipherment key data to said delivery server, and said delivery server holds said current use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses that a delivery server issues a current use key data generation request to a key management server, wherein the key management server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users, as suggested by Larsen et al. [column 1, lines 33-40].

Claim 8: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 7, and Briscoe further discloses that said key management server sets a current use key remaining effective time data*(ie. the key is changed every game-minute)* to said current use key data, and

transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use encipherment key data to said delivery server, said delivery server holds said current use encipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses*(ie. time keeper signals new game-minute)* [pages 4 & 5, paragraphs 71 & 80].

Claim 9: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 8, and Briscoe further discloses that said delivery server issues a next use key data generating request to said key management server, when said current use key remaining effective time data becomes a first present value*(ie. time-keeper signals a new game-minute)*, said key management server generates*(ie. increments ADU index to use next key in sequence)* and holds as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data in response to said next use key data generating request, and transmits a set of said next use encipher key, said next use key identifier, and said next use key remaining effective time data to said delivery server as a next use encipherment key data, and said delivery server holds said next use encipherment key data*(ie. key managers synchronize by receiving the changing stream of ADU sequence numbers from the multicast)* [page 5, paragraphs 0080 & 0082].

Claim 10: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 9, and Briscoe further discloses that said client terminal issues a key request to a key management server*(ie. issues seed values to customer terminals)* [page 3, paragraph 0061], but does not explicitly disclose that a next use key request to said key management server when said current

use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

However, Larsen et al. discloses a similar system and further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 11: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 10, but Briscoe does not explicitly disclose that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

However, Larsen et al. further discloses that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0*(ie. current key is used until it expires)* [column 4, lines 15-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 12: Briscoe discloses the multicast delivery system according to claim 1, and further discloses a plurality of said delivery servers*(ie. multi-sender multicast)* [page 13, paragraph 0253], but does not explicitly disclose that each of said plurality of delivery server issues a next use key data generating request to said key management server while using said current use cipher key, said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, and transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and said delivery server holds said next use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses that a delivery server issues a current use key data generation request to a key management server, wherein the key management server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Furthermore, Larsen et al. discloses a delivery server issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached*

the user station must get the next network operator public key, however it will keep using the current key until it expires) [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users and give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 1, lines 33-40 & column 4, lines 15-17].

Claim 13: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 12, but Briscoe does not explicitly disclose that each of said plurality of client terminals issues a next use decipher key request to said key management server when said client terminal does not hold said current use key identifier contained in said multicast packet, said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data.

However, Larsen et al. further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in

order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 14: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 12, and Briscoe further discloses that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients*(ie. the key is changed every game-minute wherein the time keeper signals new game-minute)*, each of said plurality of client terminals issues a next use decipher key request to said key management server in response to said key data change previous notice, said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data [pages 4 & 5, paragraphs 71 & 80].

Claim 15: Briscoe discloses the multicast delivery system according to claim 1, and further discloses:

a. a plurality of said delivery servers*(ie. multi-sender multicast)* [page 13, paragraph 0253];

b. and a plurality of said client terminals*(ie. customer terminals)* [page 2, paragraph 0035];

c. a plurality of key management server*(ie. plurality of key management nodes)* [page 2, paragraph 0023];

d. but does not explicitly disclose:

i. a master server;

ii. and a plurality of slave servers, wherein each of said plurality of delivery servers issues a next use key data generating request to said master server while using said current use cipher key, said master server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and transmits a set of said next use decipher key and said next use key identifier as a next use decipherment key data to said plurality of slave servers, each of said plurality of slave servers holes said next use decipherment key data, and said delivery server holds said next use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses a master key server*(ie. network operator)* and a plurality of slave servers*(ie. user stations)*, wherein a delivery server issues a current use key data generation request to a master key server, wherein the master key server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Furthermore, Larsen et al. discloses a delivery server issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users and give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 1, lines 33-40 & column 4, lines 15-17].

Claim 16: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 15, but Briscoe does not explicitly disclose that each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers when said client terminal does not hold said current use key identifier contained in said multicast packet, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data.

However, Larsen et al. further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Briscoe with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 17: Briscoe and Larsen et al. disclose the multicast delivery system according to claim 15, and Briscoe further discloses that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients*(ie. the key is changed every game-minute wherein the time keeper signals new game-minute)*, each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers in response to said key data change previous notice, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data [pages 4 & 5, paragraphs 71 & 80].

Claim Rejections - 35 USC § 102

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-4, 18 and 19 are rejected under 35 U.S.C. 102(a) as being anticipated by AAPA (Applicant admitted prior art, pages 1-18 of Applicant's own disclosure).

Claim 1: AAPA discloses a multicast delivery system comprising:

a. a delivery server*(ie. content server)* which enciphers delivery data by using a current use cipher key to generate enciphered data and transmits a multicast packet containing said enciphered data and a current use key identifier indicative of a pair of said current use cipher key and a current use decipher key as current use keys*(ie. content server transmits packets with a key request data)* [page 2, lines 1-3];

b. a key management server*(ie. key management server)* which is connected with said delivery server through a network, holds as a current use key data, a set of said current use

decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data in response to a current use key data request [page 2, lines 4-5];

c. and a client terminal which is connected with said delivery server and said key management server through said network, receives said multicast packet from said deliver server, issues said current use key data request to said key management server to receive said current use decipherment key data from said key management server, holds said set of said current use decipher key and said current use key identifier, and deciphers said enciphered data contained in said multicast packet by using said current use decipher key when said current use key identifier contained in said multicast packet is coincident with said current use key identifier held in said client terminal*(ie. client requests key to the key management server)* [page 2, lines 4-5].

Claim 2: AAPA discloses the multicast delivery system according to claim 1, and further discloses that said delivery server generates and holds as a current use encipherment key data, a set of said current use cipher key, said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as said current use decipherment key data to said key management server, and said key management server holds said current use decipher key and said current use key identifier as said current use decipherment key data*(ie. the key management server receives a new key when the content server starts transmission)* [page 4, lines 23-26].

Claim 3: AAPA discloses the multicast delivery system according to claim 2, and further discloses that said delivery server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key

identifier, and said current use key remaining effective time data as said current use decipherment key data to said key management server, said key management server holds said current use decipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses*(ie. predetermined time interval)* [page 2, lines 3-4].

Claim 4: AAPA discloses the multicast delivery system according to claim 3, and further discloses that said delivery server generates as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data, when said current use key remaining effective time data becomes a first present value, and transmits a set of said next use decipher key, said next use key identifier, and said next use key remaining effective time data to said key management server as a next use decipherment key data, and said key management server holds said next use decipher key data*(ie. content server sends new key to key management server when the key is changed)* [page 4, lines 23-26].

Claim 18: AAPA discloses the multicast delivery system according to claim 1, and further discloses that said key management server detects a data amount of said multicast packets and charges a fee to said client terminal based on said detected data amount*(ie. subscriber contracts the charge program broadcasting)* [page 6, lines 20-24].

Claim 19: AAPA discloses the multicast delivery system according to claim 1, and further discloses that said client terminal issues said key data request to said key management server, and said key management server detects the number of said key data requests and charges a fee to said client terminal based on said detected number of key data requests*(ie.a contract*

determining section determines the existence of the subscriber contract based on the key data) [page 7, lines 11-19].

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 5-8, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Larsen et al. (7,068,791).

Claim 5: AAPA discloses the multicast delivery system according to claim 4, and further discloses that said client terminal issues a key request to a key management server*(ie. client request key to key server)* [page 2, lines 14-15], but does not explicitly disclose that a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

However, Larsen et al. discloses a similar system and further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in

order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 6: AAPA and Larsen et al. disclose the multicast delivery system according to claim 5, but AAPA does not explicitly disclose that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

However, Larsen et al. further discloses that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0*(ie. current key is used until it expires)* [column 4, lines 15-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 7: AAPA discloses the multicast delivery system according to claim 1, and further discloses the delivery server generating current use key data*(ie. the key management server receives a new key when the content server starts transmission)* [page 4, lines 23-26], but does not explicitly disclose that said delivery server issues a current use key data generating request to said key management server, said key management server generates and holds as a current use key data, a set of said current use cipher key, said current use decipher key and said current use key identifier in response to said current use key data generating request, and transmits a set of said current use cipher key and said current use key identifier as a current use encipherment key

data to said delivery server, and said delivery server holds said current use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses that a delivery server issues a current use key data generation request to a key management server, wherein the key management server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users, as suggested by Larsen et al. [column 1, lines 33-40].

Claim 8: AAPA and Larsen et al. disclose the multicast delivery system according to claim 7, and AAPA further discloses that said key management server sets a current use key remaining effective time data*(ie. predetermined time interval)* to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use encipherment key data to said delivery server, said delivery server holds said current use encipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses*(ie. the key management server needs to deliver the key to the client)* [page 2, lines 3-4 & page 5, lines 1-4].

Claim 15: AAPA discloses the multicast delivery system according to claim 1, but does not explicitly disclose:

a. a plurality of said delivery servers;

b. and a plurality of said client terminals;

c. a plurality of key management server, comprising:

i. a master server;

ii. and a plurality of slave servers, wherein each of said plurality of delivery servers issues a next use key data generating request to said master server while using said current use cipher key, said master server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and transmits a set of said next use decipher key and said next use key identifier as a next use decipherment key data to said plurality of slave servers, each of said plurality of slave servers holes said next use decipherment key data, and said delivery server holds said next use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses a master key server*(ie. network operator)* and a plurality of slave servers*(ie. user stations)*, wherein a delivery server issues a current use key data generation request to a master key server, wherein the master key server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Furthermore, Larsen et al. discloses a delivery server issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use

decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the features disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users and give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 1, lines 33-40 & column 4, lines 15-17].

Claim 16: AAPA and Larsen et al. disclose the multicast delivery system according to claim 15, but AAPA does not explicitly disclose that each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers when said client terminal does not hold said current use key identifier contained in said multicast packet, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data.

However, Larsen et al. further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in

order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

12. Claims 9-14 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Larsen et al. (7,068,791) and further in view of Briscoe (2003/0044017).

Claim 9: AAPA and Larsen et al. disclose the multicast delivery system according to claim 8, but AAPA does not explicitly disclose that said delivery server issues a next use key data generating request to said key management server, when said current use key remaining effective time data becomes a first present value, said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data in response to said next use key data generating request, and transmits a set of said next use encipher key, said next use key identifier, and said next use key remaining effective time data to said delivery server as a next use encipherment key data, and said delivery server holds said next use encipherment key data.

However, Briscoe discloses a similar system and further discloses that said delivery server issues a next use key data generating request to said key management server, when said current use key remaining effective time data becomes a first present value*(ie. time-keeper signals a new game-minute)*, said key management server generates*(ie. increments ADU index to use next key in sequence)* and holds as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data in response to said next use key data generating request, and transmits a set of said next use encipher key, said next use key identifier, and said

next use key remaining effective time data to said delivery server as a next use encipherment key data, and said delivery server holds said next use encipherment key data*(ie. key managers synchronize by receiving the changing stream of ADU sequence numbers from the multicast)* [page 5, paragraphs 0080 & 0082].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the invention disclosed by AAPA and Larsen et al. with the features disclosed by Briscoe in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 10: AAPA, Larsen et al. and Briscoe disclose the multicast delivery system according to claim 9, and AAPA further discloses that said client terminal issues a key request to a key management server*(ie. client request key to key server)* [page 2, lines 14-15], but does not explicitly disclose that a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

However, Larsen et al. discloses a similar system and further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 11: AAPA, Larsen et al. and Briscoe disclose the multicast delivery system according to claim 10, but AAPA does not explicitly disclose that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

However, Larsen et al. further discloses that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0*(ie. current key is used until it expires)* [column 4, lines 15-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 12: AAPA discloses the multicast delivery system according to claim 1, but does not explicitly disclose that a plurality of said delivery servers issues a next use key data generating request to said key management server while using said current use cipher key, said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, and

transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and said delivery server holds said next use encipherment key data.

However, Briscoe discloses a similar system and further discloses a plurality of said delivery servers*(ie. multi-sender multicast)* [page 13, paragraph 0253].

Furthermore, Larsen et al. discloses a similar system and further discloses that a delivery server issues a current use key data generation request to a key management server, wherein the key management server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Additionally, Larsen et al. discloses a delivery server issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the features disclosed by Briscoe and Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users and give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 1, lines 33-40 & column 4, lines 15-17].

Claim 13: AAPA, Larsen et al. and Briscoe disclose the multicast delivery system according to claim 12, but AAPA does not explicitly disclose that each of said plurality of client terminals

issues a next use decipher key request to said key management server when said client terminal does not hold said current use key identifier contained in said multicast packet, said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data.

However, Larsen et al. further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by AAPA with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 14: AAPA, Larsen et al. and Briscoe disclose the multicast delivery system according to claim 12, but AAPA does not explicitly disclose that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients, each of said plurality of client terminals issues a next use decipher key request to said key management server in response to said key data change previous notice, said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data.

However, Briscoe further discloses that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients*(ie. the key is changed every game-minute wherein the time keeper signals new game-minute)*, each of said plurality of client terminals issues a next use decipher key request to said key management server in response to said key data change previous notice, said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data [pages 4 & 5, paragraphs 71 & 80].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the invention disclosed by AAPA with the features disclosed by Briscoe in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17]

Claim 17: AAPA and Larsen et al. disclose the multicast delivery system according to claim 15, but AAPA does not explicitly disclose that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients, each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers in response to said key data change previous notice, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data.

However, Briscoe discloses a similar system and further discloses that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients*(ie. the key is changed every game-minute wherein the time keeper signals new game-minute)*, each of said plurality of client terminals issues a next use decipher key request to any of

said plurality of slave servers in response to said key data change previous notice, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data [pages 4 & 5, paragraphs 71 & 80].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the invention disclosed by AAPA and Larsen et al. with the features disclosed by Briscoe in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Response to Arguments

13. Applicant's arguments filed on August 22nd, 2008 have been fully considered but they are not persuasive.

Regarding Claim 1: The Applicant argues that the Briscoe reference does not explicitly disclose transmitting a current use key and a current use key identifier, as recited in the instant claim. In particular, the Applicant noted that Briscoe actually discloses transmitting a seed and not a key and further alleges that a current use key identifier is not transmitted. Furthermore, the Applicant suggests that in the instant claims, the client need not go through the step of generating a key from a seed.

The Examiner notes that while Briscoe may disclose transmitting a seed instead of a key, the seed still in fact appears to be utilized, at least indirectly*(ie. used to generate keys)*, to encrypt data in a similar fashion as the claimed invention. The Examiner further notes that the instant claim does not appear to define what exactly a "current use keys" entails, thus does not appear to expressly prohibit the act of generating a key from a seed. Therefore, the Examiner respectfully

submits that a "current use key" may be reasonably interpreted to at least encompass a seed which is indirectly used to encrypted data as well. Furthermore, the Examiner respectfully submits that Briscoe appears to suggest transmitting an identifier along with the enciphered data*(ie. preferably each encrypted data unit carries an unencrypted index number to identify to any receiver which key in the sequence should be used)* [paragraph 0026].

Additionally, the Applicant argues that the AAPA does not disclose a key management server which holds a key identifier that is indicative of a current use cipher key and current use decipher key, and further notes that the cited text does not state that the pair of keys are contained within a multicast packet.

However, the Examiner notes that AAPA discloses a key management apparatus storing keys with a corresponding publication day and time for the keys, which identify when a particular key is to be used to perform encryption; and determining which key to use by referring to the day and time required by the data encrypting apparatus [page 12, lines 12-23 of Applicant's own disclosure]. Thus, the Examiner respectfully submits that AAPA does in fact appear to disclose at least one form of a current use key identifier.

Furthermore, the Examiner respectfully submits that the instant claim does not appear to explicitly recite that a pair of keys are contained within a multicast packet along with the key identifier. The Examiner notes that, as currently recited, a current use key data set appears to comprise of a current use decipher key and a current use key identifier, thus does not appear to include a pair of key.

14. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "does not

generate a key from a seed", "a pair of keys", etc.) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
December 18, 2008
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435